KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (NY Bar #: 5590104)
ak@kazlg.com
48 Wall Street, Suite 1100
New York, NY 10005
Telephone: (800) 400-6808
Fax: (800) 520-5523

[Additional Counsel on Signature Page]

Attorneys for Plaintiff,
Keanna Curtis

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

KEANNA CURTIS, Individually and On Behalf of All Others Similarly Situated,

Plaintiff,

v.

JPMORGAN CHASE BANK, N.A.; and EARLY WARNING SERVICES, LLC D/B/A ZELLEPAY.COM,

Defendants.

Case No.: 1:22-cv-10286

CLASS ACTION COMPLAINT FOR:

1) **VIOLATIONS OF THE ELECTRONIC FUND TRANSFER ACT ("EFTA");**
2) **BREACH OF CONTRACT;**
3) **UNJUST ENRICHMENT;**
4) **NEGLIGENCE;**
5) **NEW YORK GENERAL BUSINESS LAW §§ 349 & 350**

PLAINTIFF DEMANDS TRIAL BY JURY

Plaintiff Keanna Curtis ("Ms. Curtis" or "Plaintiff") brings this complaint, by and through her attorneys and on behalf of all others similarly situated, against Defendants JPMorgan Chase Bank, N.A. ("Chase Bank," or the "Bank") and Early Warning Services, LLC d/b/a Zellepay.com ("Zelle") (together the "Defendants") and alleges:

INTRODUCTION

1. The Zelle money transfer system is rife with fraud—fraud that places all Zelle users at an acute and immediate risk. Billions of dollars of fraudulent transactions are processed by the service each year. Victims of Zelle fraud, like Plaintiff, are often left devastated by such fraud, which can drain hundreds or thousands of dollars from their bank accounts.

2. But when Zelle fraud victims turn to Chase Bank for help, the Bank has a simple, repeated, bad faith response: it is your fault, you are on your own, and we will not help.

3. The Bank's corporate policy of "blaming the victim" is good business for the Bank. As a partial owner of Zelle (along with several other of America's largest banks), the Bank has a huge incentive to get as many consumers as possible to sign up for and use Zelle for payments and money transfers: the more consumers it can persuade to set up an account and use Zelle, the more money the Bank saves by avoiding transaction payments to *other* payment networks. Accordingly, the Bank works with Zelle to aggressively market the Zelle service to consumers and accountholders alike, urging them to sign up for Zelle every time they log in to online banking, use the Bank's mobile app, or even visit a Chase ATM.

4. But the marketing of Zelle by Defendants, including during the quick, rushed sign up process for Zelle in the Bank's mobile app or website, contains materially deceptive representations suggesting that Zelle is safe, while omitting any warnings

regarding the acute and immediate risk of fraud. Those representations and omissions, which Plaintiff relied upon, are false and misleading.

5. Zelle too knows that fraud on its service is rampant, and it is on notice of consumers' claims, but consumers are similarly left without recourse from Zelle, just like Chase Bank.

6. Unlike other commonly used consumer payment systems—credit cards, debit cards, even PayPal—***Zelle has no consumer fraud protections, money transfers are immediate and irrevocable, and neither Zelle nor the Bank will provide help in the case of fraud***. These material facts about Zelle are omitted from marketing about Zelle promulgated by Defendants for a simple reason: no reasonable consumer would sign up for and use the service if these facts were fairly disclosed.

7. Having lured Chase Bank accountholders to sign up for and use the Zelle service with deceptive and incomplete marketing promises, Defendants fail victims of Zelle fraud in two distinct ways.

8. First, for victims of Zelle fraud who had their access devices used by fraudsters, the Bank maintains a massive bureaucratic apparatus designed to make it impossible for victims to lodge a successful fraud claim. When such victims make a claim for fraud, the Bank denies the claim without conducting a full investigation and blames fraud victims for the fraud. As occurred with Plaintiff, the Bank summarily rejected fraud claims without explanation or recourse.

9. Second, for victims of Zelle fraud who were tricked into making fraudulent transfers to fraudsters, the Bank has adopted a practice wherein any and all such fraud reimbursement claims are denied in their entirety—with a cursory investigation and denial of reimbursement— another instance of the Bank's "blame the victim" corporate policy.

10. In both circumstances the consumer, not Chase Bank or Zelle, is left without recourse following the fraud or unauthorized transaction by a third-party.

11. These policies and practices contradict Defendants' marketing promises.

12. These policies and practices also violate the Electronic Fund Transfer Act ("EFTA"), a statute with the purpose of "provid[ing] a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems." § 1693(b). "The primary objective of [the EFTA] is the provision of individual consumer rights." *Id.*

13. These policies and practices also breach contractual promises the Bank made and violate the duty of care owed, as discussed in detail below.

14. Plaintiff and the Class members have been injured by signing up for and using Zelle. Plaintiff brings this action on behalf of herself, and the putative Class, because Plaintiff should not be left "holding the bag" for fraudulent transactions.

15. Plaintiff seeks actual damages, punitive damages, restitution, and an injunction on behalf of the general public to prevent Chase Bank and Zelle from continuing to engage in their illegal practices presently and in the future as described herein.

JURISDICTION AND VENUE

16. Original subject matter jurisdiction is valid in the U.S. District Court pursuant to 28 U.S.C. § 1331 because this case arises out of violations of federal law under the EFTA, 15 U.S.C. §§ 1693, *et seq*. Jurisdiction of this Court arises pursuant to 28 U.S.C. §§ 1331 and 1367 for supplemental jurisdiction over the common law claims.

17. The Court also has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because (i) there is minimal diversity; (ii) Defendants are not government entities against whom the District Court may be foreclosed from ordering relief; (iii) there are more than one hundred (100) people in the putative classes; and (iv) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

18. Venue is proper pursuant to 28 U.S.C. § 1391(b) because: (1) Defendants transact business within this judicial district, Chase Bank has its principal place of business in New York City, New York, and a substantial part of the events giving rise to Ms. Curtis's cause of action against Defendants arise in this judicial district; and (2) Defendants' contacts with this District are sufficient to subject them to personal jurisdiction within this judicial district for Plaintiff's causes of action. Additionally, there is at least pendent personal jurisdiction over Zelle for Plaintiff's claims.

PARTIES

19. Ms. Curtis is a natural person, individual citizen and resident of New York, County of Nassau.

20. Upon information and belief, Chase Bank is a nationally-chartered bank with its principal place of business in New York City, New York, which is within this judicial district.

21. Plaintiff is informed and believes, and thereon alleges, that Zelle is a limited liability company established under the laws of Delaware with its principal place of business in the State of Arizona.

22. Zelle is a money payment platform ("MPP") that facilitates peer-to-peer ("P2P") instant payment services. Zelle is owned by seven of America's largest banks, which includes Defendant Chase Bank.

23. Upon information and belief, Zelle earns money for its owners and saves participating banks money by minimizing the fees the banks are charged for competitor P2P payment transactions.

ZELLE – THE FAVORITE APP OF FRAUDSTERS

24. Created in 2017 by America's largest banks[1] to enable digital money transfers, Zelle now comes embedded in Chase's banking app, or as a stand-alone service available on the Zelle website and is now America's most widely used money transfer service, outpacing its closest rival (Venmo) by $260 billion in transfers in 2021.[2]

25. About 1.8 billion payments—totaling $490 billion—were sent by consumers and businesses through the Zelle Network in 2021, according to Early Warning Services. Total dollars transferred were up 59% from 2020.[3]

26. Nearly 18 million people have been victims of "widespread fraud" on money transfer apps, according to a letter sent in late April of 2022 to Zelle by U.S. Senators Elizabeth Warren of Massachusetts, Robert Menendez of New Jersey, and Jack Reed of Rhode Island.[4]

27. "Zelle's biggest draw—the immediacy of its transfers—also makes scams more effective and 'a favorite of fraudsters,' as consumers have no option to cancel a transaction even moments after authorizing it," the letter stated.

28. The 1500 banks and credit unions who are members of the Zelle network, including Chase Bank, know full well that they have a widespread fraud problem on

---

[1] JPMorgan Chase, Bank of America, Capital One, PNC, BB&T (now Truist), U.S. Bank and Wells Fargo.

[2] Cowley, Stacy & Nguyen, Lananh, "Fraud is Flourishing on Zelle. The Banks Say It Is Not Their Problem," *New York Times* (March 6, 2022), https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html (last visited September 13, 2022).

[3] ZellePay.com, *Nearly Half a Trillion Dollars Sent by Consumers and Businesses with Zelle in 2021* (February 02, 2022), https://www.zellepay.com/press-releases/nearly-half-trillion-dollars-sent-consumers-and-businesses-zelle-2021 (last visited September 21, 2022).

[4] Letter from Elizabeth Warren, Robert Menendez, Jack Reed, Sen., U.S. Cong., to Al Ko, CEO, Early Warning Services (April 2, 2022).

their hands but have misrepresented and failed to take steps to warn their accountholders of these risks—or to protect their accountholders who fall prey to fraud.

29. Consumers are not aware that money transfer transactions with Zelle differ from other money transfer platforms.

30. Nor are consumers aware that the Zelle network has become a preferred tool for fraudsters. Fraudsters and scammers have turned to Zelle as their favorite service because transfers are immediate and unrecoverable. Zelle has an additional design feature that makes it a fraudster's favorite: one can become a Zelle user and recipient without revealing their true identity.

31. Led by Idaho Attorney General Lawrence Wasden and Oregon Attorney General Ellen Rosenblum, a bipartisan coalition of thirty-three (33) attorneys general wrote the Consumer Financial Consumer Protection Bureau ("CFPB"), calling for stronger consumer safeguards for money sharing platforms and apps like Zelle. The letter, written in response to the CFPB's request for comments on its inquiry into "Big Tech Payment Platforms," noted a rise in complaints against popular payment apps including Zelle. The letter highlighted that: "[m]any consumers have been scammed out of hundreds or thousands of dollars by other users of these payment platforms [like Zelle]. ***Scammers are attracted to real-time payment platforms, in large part, because they do not need to reveal their true identity to set up an account"*** (emphasis added).

32. As a result, crooks are using Zelle to rob consumers when listing fake puppies for sale, advertising phony apartments or homes to rent, threatening utility service cut-off without immediate transfer of money, or offering extra income for wrapping a personal car in an advertisement.[5]

[5] Letter from Ellen F. Rosenblum Oregon Attorney General, and Lawrence Wasden, Idaho Attorney General to Rohit Chopra, Director, Consumer Financial Protection

33. A common version of the employment scam involves fraudsters, posing as potential employers, initially contacting individuals via text message, then through a live interview. The fraudsters proceed to "hire" the individual, give them a faulty check to deposit in their bank, and transfer them the money back through Zelle for office supplies.

34. Another common scam: a prospective buyer supposedly wants to buy an item listed on Facebook Marketplace but then claims that the seller needs to upgrade their Zelle app to accept money from their "business account" for the big-ticket purchase to go through, according to a June 2022 alert by the Better Business Bureau. The scammer supposedly puts up $300 and sends you screenshots of their Zelle app as proof. Then, the scammer pressures you into paying them back.[6]

35. "Scammers go where it's easy to get the money. Zelle is their current mechanism to drain consumer accounts," warned Ed Mierzwinski, PIRG Education Fund's senior director of federal consumer programs. "The scammers are taking advantage of consumers because the banks are letting them," Mierzwinski said. "My basic advice is don't use these apps."[7]

Bureau (December 20, 2021), https://www.doj.state.or.us/wp-content/uploads/2021/12/State-Attorneys-General-Comment-on-CFPBs-Inquiry-into-Big-Tech-Payment-Platforms-2021.pdf (last accessed September 21, 2022).

[6] Better Business Bureau, *BBB Scam Alert: Crafty New Scam Targeting Facebook Marketplace Sellers* (June 24, 2022), https://www.bbb.org/article/scams/27212-scam-alert-how-to-spot-shady-buyers-on-facebook-marketplace (last accessed September 21, 2022).

[7] Tompor, Susan, *DTE Impersonators Drained Rochester Hills Woman's Checking Accounting Using Zelle App*, Detroit Free Press (June 30, 2022), https://www.freep.com/story/money/personal-finance/susan-tompor/2022/06/30/utility-shutoff-scam-stole-cash-via-zelle/7714138001/ (last accessed Sept. 21, 2022).

36. The fraud risk is so acute and immediate that if consumers use Zelle, PIRG recommends that consumers maintain a separate bank account to link to Zelle accounts.

37. Scams like these are rampant on the Zelle network precisely because of Zelle's design and architecture, specifically that money transfer is instantaneous and unrecoverable. Indeed, there is virtually no recourse for consumers to recoup losses due to fraud, unlike other payment methods commonly used by American consumers—debit cards, credit cards, and even Venmo.

38. The unique, misrepresented, and undisclosed architecture of the Zelle payment system, the financial relationship between Chase Bank, and Chase Bank's own policies specific to Zelle transactions means—again, unlike other payment options commonly used by American consumers—that virtually any money transferred for any reason via Zelle is gone forever, without recourse, or reimbursement protection for victimized accountholders.

39. Defendants did nothing to stop the problem or sufficiently warn users of the problem prior to the harm caused to Plaintiff, for fear of suppressing new users and use of the service by existing users and because of Defendants' financial interests.

40. ABC7 News reports that one longtime Chase Bank customer was tricked by a fraudster out of $7,000 through Zelle.[8]

41. Not until recently did Defendants begin providing warnings prior to Zelle transfers to its accountholders regarding the risks of using the service and regarding common scams to be on alert for. However, on information and belief, Chase Bank provided none of these warnings in its Zelle marketing, much less prior to each Zelle transfer or prior to the harm suffered by Plaintiff as alleged herein.

[8] https://abc7news.com/zelle-scam-chase-bank-refunds-zell-bofa/11317729 (accessed on October 17, 2022)

42. Defendants' warnings are still inadequate to protect consumers, in part, because Defendants continue to market Zelle in a way that suggests it is safe to use.

43. In October 2022, Senator Elizabeth Warren's office published a report titled, "Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It" ("Warren Report").[9] The Executive Summary of the Warren Report states as follows:

> In April 2022, Senator Warren opened an investigation of Zelle and its owner and operator, Early Warning Services, LLC (EWS), after numerous reports indicated that Zelle is a preferred tool of fraudsters and bad actors who abuse Zelle's instantaneous, easy-to-exploit transfers to defraud consumers. Zelle and EWS are owned and operated by a consortium of big banks, who initially refused to turn over any significant information on the extent of fraud on the platform.
>
> At a September 2022 Banking Committee hearing, Senators Warren and Menendez continued to press the banks for this information, and received a commitment from several CEOs that they would provide it to Congress. While JPMorgan Chase and several other banks still refused to make key information about fraud public, several others did provide the information. This report contains the findings of Senator Warren's review of data received to date. It finds that:
>
> - **Fraud and theft are rampant on Zelle – and are increasing.** The big banks that own Zelle market the product by telling their customers that the platform is safe and secure. … EWS, Zelle's parent company, brands itself as "innovative," "collaborative," and "trustworthy." But PNC Bank reported that the number of fraud and scam claims from customers increased from 8,848 in 2020, to a pace of over 12,300 in 2022. Similarly, U.S. Bank reported 14,886 fraud and scam claims on Zelle in 2020, and that its customers are on pace to report nearly 45,000 claims in 2022.

[9] Accessible at: https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf (last visited October 18, 2022).

The four banks that reported the relevant data received scam and fraud claims in excess of $90 million in 2020, and are on pace to receive scam and fraud claims in excess of $255 million in 2022.

- **Banks are not repaying the vast majority of cases where customers were fraudulently induced into making payments on Zelle.** Overall, four banks reported 192,878 cases of scams – cases where customers reported being fraudulently induced into making payments on Zelle – involving over $213.8 million of payments in 2021 and the first half of 2022. In the vast majority of these cases, the banks did not repay the customers that were defrauded. Overall the three banks that provided full data sets reported repaying customers in only 3,473 cases (representing 9.6% of scam claims) and repaid only $2.9 million (representing 11% of payments).

- **Banks are not repaying customers who contest "unauthorized" Zelle payments – potentially violating federal law and CFPB rules.** Zelle claims to have a "zero liability policy" for cases in which a bad actor gains access to a consumer's Zelle account and uses it to make unauthorized payments, and the Electronic Fund Transfer Act (EFTA) and the Consumer Financial Protection Bureau's (CFPB) "Regulation E" require that the banks repay customers when funds are illegally taken out of their account without authorization. But the data provided by the banks revealed that they reimbursed consumers for only 47% of the dollar amount of cases in which customers reported unauthorized payments on Zelle in 2021 and the first half of 2022.

44. Thus, the Warren Report explains the very same facts alleged here: that major banks that own Zelle—including Chase Bank—have given consumers the false impression that (1) the Zelle services that they offer are safe and free from fraudulent transactions; (2) Chase Bank will reimburse its customers for fraudulent charges when, in fact, it largely refuses to do so; (3) Chase Bank and Zelle know the fraudulent transactions are, in fact, fraud, and not authorized transactions conducted

by the Chase Bank account holders; (4) Defendants are aware that fraudulent transactions conducted through Zelle are increasing dramatically in frequency; and (5) Defendants have failed to implement or maintain adequate safeguards to prevent fraudulent transactions conducted through Zelle.

45. The Warren Report further corroborates the allegations in this complaint that Chase Bank owns and profits from Zelle, that Zelle (and, in turn, Chase Bank by offering Zelle to its customers) and Chase Bank encourage customers to utilize Zelle's service for Defendants' own profit/gain:

> Zelle's parent company, EWS, is owned and operated by seven of the U.S.' largest banks: JPMorgan Chase… EWS markets Zelle as "the fast, safe and easy way to send and receive money." The company encourages banks and credit unions to join the Zelle Network and offer the product to consumers as part of their wider suite of banking services. Indeed, EWS pitches Zelle to the nation's banks and credit unions with data suggesting that "customers using Zelle are more profitable and stay with the financial institution longer" than customers who do not use Zelle. In other words, when banks adopt and offer Zelle and their customers use it, banks profit. According to EWS, banks that offer Zelle to customers save on management costs, earn on customer retention and greater engagement with banking products and services, and "maintain a central role in [customers'/members'] financial lives." It is in banks' financial interest for consumers to use Zelle. So, while EWS is marketing the Zelle Network to financial institutions, those financial institutions are marketing Zelle to their customers …. big banks that own Zelle market the product by telling their customers that the platform is safe or secure. …

46. Moreover, the Warren Report calls out Chase Bank for not being transparent by stating:

> JPMorgan Chase has refused to make public the complete data on Zelle fraud and scams, even after its CEO, Jamie Dimon, publicly promised before Congress that his company would provide it.

47. Despite its awareness of consumer fraud on Zelle, Defendants have knowingly, intentionally, and willfully refused to refund its customers for such fraudulent transactions.

THE FALSE AND MISLEADING ZELLE SIGN-UP PROCESS LURES ACCOUNTHOLDERS TO SIGN UP FOR AND USE ZELLE

48. It is free to sign up with Zelle, and Zelle is integrated into Chase Bank's websites and mobile app.

49. To banks, Zelle advertises itself as a way to grow and retain customers, to reduce cash and check management costs by digitizing payments, and to create more cross-selling opportunities that help banks' profitability.

50. To consumers, Zelle advertises itself as providing users with access to money right away, as a "a fast, safe and easy way to send and receive money with friends, family and others you trust – no matter where they bank."[10] Further, "[o]nce you're enrolled with Zelle, all you need is an email address or U.S. mobile phone number to send money to friends and family straight from your banking app."[11]

51. Many Chase Bank accountholders sign up for Zelle after they have been Chase Bank accountholders for years—often by virtue of their status as accountholders who wish to use Chase Bank's online banking services.

52. During the Zelle sign-up process, Chase Bank accountholders are not affirmatively provided with agreements or disclosures previously provided at the time they opened their Chase Bank account.

53. For all Chase Bank accountholders and users of Zelle, whether signed up directly with Zelle or by mere use of their Chase Bank account, Chase Bank and Zelle agreed to provide electronic fund transfer services.

---

[10] https://www.zellepay.com/security (last accessed November 16, 2022).
[11] https://www.zellepay.com/how-it-works (last accessed Nov. 22, 2022).

54. Absent agreement by Chase Bank and Zelle to provide electronic fund transfer services, the transactions at issue in this lawsuit would not have occurred.

55. Chase Bank and Zelle tell consumers that all they need to send or receive money through Zelle is an email address or a valid U.S. mobile phone number. Though this fact is conveyed to consumers under the guise of showcasing Zelle's simplicity, in actuality, Zelle requires a valid email address or U.S. mobile phone number as a condition of Zelle providing its electronic fund transfers services. Indeed, a valid email address or U.S. mobile phone number is the access device issued by Zelle for consumers to initiate electronic fund transfers.

56. Chase Bank also issues access devices to accountholders to complete Zelle transactions by means of their U.S. checking or savings account verification information.

57. Chase Bank's mobile app and online banking website feature numerous invitations and advertisements to sign up for the Zelle service. Defendants' advertisements and marketing for Zelle, however, are not limited to mobile apps and online banking; they also advertise Zelle at Chase ATMs, on billboards, and by other means. Upon information and belief, such marketing is jointly designed and promulgated by Defendants for their mutual benefit.

58. Chase Bank gives consumers the false impression that Zelle is safe when promoting Zelle as an integrated service with its mobile banking application and representing that Zelle is fast, easy, convenient and secure. Specifically, in its online marketing about Zelle, Chase Bank makes promises that Zelle (which the Bank previously referred to as "Chase QuickPay with Zelle") is "a fast, easy and convenient way to send and receive money …"[12] Moreover, Chase Bank advertises

[12] https://www.chase.com/personal/zelle (accessed on October 17, 2022).

Zelle, both online and during the Zelle signup process within the Bank's mobile app or website, as a "secure" service.[13]

59. At best, in describing the Zelle service on Chase Bank's website, the website states: "Make sure you send money to people you know and trust in order to help avoid scams and protect your account" and "We don't protect or cover purchases if you use Zelle® to pay for goods or services."[14] Those statements, while inadequate to inform consumers that Zelle operates differently from other payment options commonly used by American consumers such as Venmo or Paypal and thus have different risks, are noticeably absent from the Zelle signup process within Chase Bank's mobile application.

60. Prior to the fraudulent losses incurred by Plaintiff and the Class Members, at no time did Chase Bank, through its marketing or during Chase Bank's sign-up process, warn Plaintiff and the Class Members of the true security risks of using the Zelle service—including the immediate and acute risk of fraud, the dangerous architecture of the system and the risk that fraudulent losses will never be reimbursed by Defendants.

61. The Bank misrepresents (and omits facts about) the true nature, benefits, and risks of the Zelle service, which means that users are at risk of fraud when using Zelle. Had Plaintiff been adequately informed of these risks, she would not have signed up for or used Zelle.

62. Defendants' marketing and representations about Zelle—including within its app and website—misrepresented and never disclosed these risks and material facts, instead luring consumers to sign up for and use the service with promises of ease, convenience and security.

---

[13] *Id.*
[14] *Id.*

63. Defendants' misrepresentations and omissions are especially pernicious because Defendants alone know material facts regarding Zelle—including the rampant fraud and theft of accountholders' money, the details concerning the fraudulent transactions and the parties to such transactions, and the fact that fraud-induced Zelle transfers will almost never be reimbursed by Defendants.

FALSE AND MISLEADING ZELLE MARKETING

64. Zelle advertises its money transfer services to consumers by claiming that it is "a fast, safe and easy way to send and receive money." It also urges consumers to use Zelle to "[s]afely send money to friends and family, no matter where they bank,[15] [16]and that consumers can "use Zelle to safely send and receive money straight from your banking app."

65. Zelle encourages consumers to "pay it safe" by "look[ing] for Zelle in your banking app[.][17]"

66. Defendants tout Zelle to accountholders as a secure, free and convenient way to make money transfers. However, the marketing (including during the sign-up process) misrepresents and omits a key fact about the service: there is virtually no recourse for consumers or accountholders to recoup losses due to fraud. Indeed, unlike virtually every other payment method commonly used by American consumers—debit cards, credit cards, and even PayPal—there is no protection for accountholders who are victims of fraud.

67. The unique, misrepresented, and undisclosed architecture of the Zelle payment system means that virtually any money transferred for any reason via Zelle

---

[15] "*See* ZellePay.com, *How Zelle Works*, https://www.zellepay.com/how-it-works (last visited August 17, 2022).

[16] *See* https://www.zellepay.com (last visted on October 19, 2022).

[17] *See* ZellePay.com, *How to Pay it Safe with Zelle* https://www.zellepay.com/financial-education/pay-it-safe (last visited August 17, 2022).

is gone immediately and forever, without recourse, reimbursement, or protection, and this information is omitted during the Zelle sign-up process. Even Defendants' online advertising does not adequately inform consumers that Zelle operates unlike other payment options commonly used by American consumers such as Venmo or PayPal.

68. Worse, Defendants misrepresent and omit the truth about a practice they have adopted: They do not and will not reimburse Zelle users for losses when they are tricked into compromising their access devices and making Zelle transfers due to fraud and will almost never reimburse Zelle users for losses when access devices are stolen and their Zelle accounts are preyed upon by fraudsters—even where those losses are timely reported.

69. Defendants were required to accurately represent the unique features of the Zelle service in their marketing about it and in contractual representations. But they failed to do so.

70. As a result, users like Plaintiff signed up for and used the Zelle service without the benefit of complete, accurate information regarding that service, and later ended up with huge, unreimbursed losses due to fraud. Such users never would have signed up for Zelle if they had known the extreme risks of using the service.

71. The acute and immediate risks described above are well known to Defendants but were omitted from all of their Zelle marketing to Plaintiff and the Class Members.

72. On information and belief, the Bank uses Zelle, which it owns in part, to insulate itself from financial liability for fraudulent and unauthorized transactions, which saves the Bank money.

DEFENDANTS HAVE IGNORED REGULATORY GUIDANCE

73. Recent CFPB guidance on unauthorized Electronic Fund Transfers ("EFTs") indicates P2P payments are EFTs, such as transactions made with Zelle, and trigger

"error resolution obligations" to consumers to protect them from situations where they are fraudulently induced and requested by a third party to provide their account information that results in authorized debits from their accounts.[18]

74. Additionally, the Federal Deposit Insurance Corporation ("FDIC") issued a report in March 2022 finding that Regulation E's "liability protections for unauthorized transfers apply even if a consumer is deceived into giving someone their authorization credentials."[19] Further, the FDIC stated that "[c]onsumer account disclosures cannot limit protections provided for in the regulation."[20] The FDIC stated that both the banks and MPPs are considered "financial institutions" under Regulation E, and as such have investigative and error resolution obligations under Regulation E.

75. Even with this regulatory guidance, Defendants have not changed course and provided protections for fraud.

76. On information and belief, Defendants do not reimburse consumers for losses from unauthorized EFTs due to Zelle fraud, even where the losses are timely reported by consumers.

77. On information and belief, Chase Bank has notified Zelle of each loss sustained by the Plaintiff and the putative class members, but Zelle has not complied with its "error resolution" obligations or investigated any of the unauthorized EFTs,

---

[18] Consumer Financial Protection Bureau, *Electronic Fund Transfers FAQs*, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last visited August 17, 2022).

[19] FDIC, *Consumer Compliance Supervisory Highlights Federal Deposit Insurance Corporation* (March 2022), https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2022.pdf (last accessed Sept. 21, 2022).

[20] *Id.*

and Zelle has failed to reimburse any of the unauthorized EFTs. Instead, Zelle's practice is to refer consumers back to Chase Bank.

78. Chase Bank has not complied with its "error resolution" obligations, fails to complete proper investigations, and has failed to reimburse any of the unauthorized EFTs.

CHASE BANK BREACHES CONTRACT PROMISES AND THE IMPLIED COVENANT

79. The Bank's Deposit Account Agreement ("Agreement 1") applicable to consumer accounts promises users that if they timely report fraud, such fraud will be fairly investigated and accountholders will not be liable for fraudulent transfers.

80. Zelle is never mentioned by name, in the Agreement 1 that accountholders receive when opening a Chase Bank account, including in the version with Effective date "3/20/2022." Nor is Zelle mentioned in the Agreement 1 with the Effective date of "10/16/2022", which upon information and belief is the current version of Agreement 1.

81. Under the heading "In case of errors or questions about your electronic funds transfers," Agreement 1 for personal accounts states:

> We must hear from you NO LATER than 60 days after we sent you the FIRST statement on which the error appeared. Please provide us with the following:
>
> Your name and account number;
> A description of the error or the transaction you are unsure about, and why you think it is an error or want more information; and
> The amount of the suspected error.
>
> We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. However, if we need more time, we may take up to 45 days to investigate your complaint or question. If we do this, we will credit your account within 10 business days for the amount you think is in error, so that you will

> have the use of the money during the time it takes us to complete our investigation. If your first account deposit is less than 30 days before the date of the suspected error, the 10-business-day period is extended to 20 business days. If your first account deposit is less than 30 days before the date of the suspected error or the transaction occurred at a point-of-sale location or outside the U.S., the 45-day period is extended to 90 days.
>
> If you call us, we may require that you send us your complaint or question in writing within 10 business days. If we do not receive it within 10 business days, we may not credit your account.
>
> We will tell you the results within three business days after completing our investigation.

See Agreement 1, at Page 13.

82. Chase Bank's "Online Service Agreement For Consumer Customers With Checking Accounts or Asset Management Accounts or Home Equity Lines of Credit, with or without other non-checking accounts" ("Agreement 2"), with a stated Effective date of "09/13/2020", under the heading "Your Liability for Unauthorized Transfers or Payments" states:

> If you permit other persons to use Payments and Transfers or your Password, you are responsible for any transactions they authorize from your accounts. **If you believe that your Password has been lost or stolen or that someone has made payments, transferred or may transfer money from your account without your permission, notify us AT ONCE, by calling 1-877-242-7372 (J.P. Morgan Online clients only, call 877-840-0723) or writing us at Online Customer Service, P. O. Box 2558, Houston, TX 77252-9968**.
>
> Tell us AT ONCE if you believe your Password has been lost or stolen or that an unauthorized transfer or payment has been made from any of your deposit or prepaid accounts. Telephoning us is the best and fastest way of keeping your possible losses to a minimum. If you do not do so, you could lose all the money in each of the accounts, as well as all of

> the available funds in any overdraft protection account or any other credit line included among your accounts. If you tell us within two (2) Business Days after you discover the loss or theft, you are completely covered if someone makes a transfer or payment without your authorization.
>
> If you do not tell us within two (2) Business Days after you discover the loss or theft of your Password or that an unauthorized online transfer or payment has been made from any of your deposit or prepaid accounts, and we can prove we could have stopped someone from making a transfer or payment without your authorization if you had told us, you could lose as much as $500. Furthermore, if any account statement shows online transfers or payments that you did not make, tell us AT ONCE. If you do not tell us within sixty (60) days after a statement showing such a transfer or payment was transmitted to you, you may not get back any money you lost after the sixty (60) days if we can prove that we could have stopped someone from taking the money if you had told us in time.
>
> If a good reason, such as a long trip or hospital stay, kept you from telling us, we will extend the time periods.

See Agreement 2, at Section 30.1 (emphasis in original).

83. Additionally, the Agreement 2 under the heading "Our Guarantees" states:

> In the event that money is removed from your consumer deposit accounts (i.e., checking or savings) or prepaid accounts with us without your authorization through Payments or Transfers, we will reimburse you 100% if you tell us within two Business Days of your discovery of the unauthorized transaction. (See the paragraph entitled "Your Liability for Unauthorized Transfers or Payments", above governing "Your Liability for Unauthorized Transfers.")

See Agreement 2, at Section 31.1.

84. Moreover, Chase Bank's Zelle Service Agreement and Privacy Notice ("Agreement 3"), with an effective date "5/23/2021", which upon information and belief is the current version of Agreement 3, states under the heading "Errors and

Questions about Service: For Transfers From Consumer Deposit Accounts and Chase Liquid Cards Only":

> If you think your statement is wrong, or if you need more information about a transaction listed on it, call or write us at the telephone number or address at the end of this Agreement.
>
> We must hear from you NO LATER than 60 days after we sent you the FIRST statement on which the error appeared. Please provide us with the following:
>
> Your name and account number;
> A description of the error or the transaction you are unsure about, and why you think it is an error or want more information; and
> The amount of the suspected error.
>
> We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. However, if we need more time, we may take up to 45 days to investigate your complaint or question. If we do this, we will credit your balance within 10 business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If you opened your account less than 30 days before the date of the suspected error, the 10-business-day period is extended to 20 business days. If you opened your account less than 30 days before the date of the suspected error or the transaction occurred at a point-of-sale location or outside the U.S., the 45-day period is extended to 90 days.
>
> If you call us, we may require that you send us your complaint or question in writing within 10 business days. If we do not receive it within 10 business days, we may not credit your balance.
>
> We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation.

See Agreement 3, at Section 20.

85. None of these three agreements specify whether Zelle transfers are governed

by Regulation E.[21] Accordingly, none of the Agreements and no correspondence by Zelle or the Bank to consumers informs consumers of Zelle's obligation as a "financial institution" under Regulation E.

86. The term "unauthorized" reasonably encompasses all transactions occurring as a result of fraud. In other words, no fraud-induced transaction can reasonably be considered "authorized."

87. As alleged with specificity herein, Chase Bank breached the Agreements, because Chase Bank adopted an unreasonable and unfair understanding of the Agreement's term "unauthorized."

88. The Bank unfairly and improperly considers Zelle transactions induced by fraud to be "authorized," thus shirking fraud protection promises it otherwise makes in the Agreements or that are required by law.

89. The Bank requires that all accountholders participating in online banking "agree" to Agreement 3, under which the accountholder purportedly agrees to indemnify Zelle.

90. Yet, whenever accountholders file claims directly with Zelle, Zelle refuses to properly investigate, reverse or reimburse accountholders.

91. On information and belief, even where the Chase Bank accountholder, like Plaintiff, has not made a claim directly with Zelle, Zelle knows about the claim, yet fails to take any investigative or remedial action.

---

[21] The only reference to Zelle in Agreement 2 states: "Certain payments or transfers available through the Online Service may be subject to terms and conditions in agreements separate from this Agreement that apply to such other services including, but not limited to, the online wire transfer service; payroll and tax payment services, the Chase QuickPay®with Zelle® Service and Terms for Your Chase Pay® Wallet. Please refer to the agreements and documentation that you receive for those services for that information." However, that document does not identify any website address or other means for Plaintiff and Class Members to locate any separate agreement that may govern Zelle transactions.

PLAINTIFF'S FACTUAL ALLEGATIONS

92. When Ms. Curtis signed up for Zelle, she was not informed by either defendant that Zelle's service had a significant "catch" and that significant monetary losses could result from signing up for the service—or that those losses are almost never reimbursed by Defendants.

93. Ms. Curtis is a young college student who was searching for a new job where she could work remotely to accommodate her school schedule.

94. On or about April 20, 2022, Ms. Curtis was searching online for a new job and believed she found one when she received a text message from an individual who went by the name of Max Segura for a remote position at "Work Fusion."

95. Ms. Curtis was interested in the purported remote position and began communicating with said individual (a fraudster) who instructed her to download a messenger application called Telegram Messenger.

96. On or about April 21, 2022, Ms. Curtis downloaded that mobile application and shortly after began having a conversation with an individual who went by the name of Ronald Hutchinson.

97. After approximately an hour of speaking with this individual (another fraudster), Ms. Curtis was informed that she was hired for a position as Administrative Assistant and informed her that she would receive an email from the company that would contain a check of $1,422. Ms. Curtis was directed to resize and print the check using the direct deposit feature through the Chase Bank mobile application to pay for equipment and software for her position. Ms. Curtis was directed to screenshot the entire process. In addition, the fraudster stated that a physical check of $150 would be sent to her through the mail as a sign-on bonus.

98. Ms. Curtis was uncertain about the instruction of resizing and depositing the check, which led her to looking up "Work Fusion" online. After locating a Work Fusion YouTube, Twitter, Glassdoor, and LinkedIn page, Ms. Curtis felt reassured

that she was applying for a legitimate position.

99. As the fraudster requested, Ms. Curtis resized, printed, and deposited the $1,422 check. Chase Bank only released $500 and emailed Ms. Curtis to inform her that the remaining balance would be released the next day.

100. Following the deposit of the check, the individual who went by the name of Mr. Hutchinson further instructed Ms. Curtis to send the funds to someone that goes by the name of Castano Penn, the person who was supposedly in charge of purchasing and sending Ms. Curtis the equipment and software for her position. Ms. Curtis was instructed by the "employer" to send money through Zelle. Ms. Curtis sent the $500 to the fraudster via the Zelle feature in Chase Bank's mobile banking application. Mr. Hutchinson subsequently requested Ms. Curtis pay the remainder of the check from her personal funds until the entire balance was released the next day, but Ms. Curtis declined to do so.

101. Prior to the Zelle transaction, Ms. Curtis was not provided an adequate warning from Chase Bank or Zelle about fraud risks.

102. The next day, on or about April 22, 2022, Ms. Curtis continued conversing with Mr. Hutchinson and sent the remaining $900 to him through Zelle in Chase Bank's mobile app. However, Ms. Curtis received an error message. Prior to checking her account, Ms. Curtis followed Ms. Hutchinson's instructions to send an additional $500 to him because of an alleged error from the previous transaction.

103. Later that day, the individual who went by the name Mr. Hutchinson stated that the first payment was not enough. He sent her a $2,125 check that included Ms. Curtis's signing bonus and the additional $500. When Ms. Curtis deposited the second check, Chase Bank informed her that the funds were on hold until May 3. At this point, Ms. Curtis realized that she had been a victim of fraud.

104. That same day, after realizing the fraud, Ms. Curtis timely called and informed Chase Bank of the fraud and reported the unauthorized electronic fund

transfer. Chase Bank's representative told Ms. Curtis not to worry and to send screenshots of her conversation with the fraudsters. Ms. Curtis sent Chase Bank over eighty-two pages of her conversations with the fraudsters.

105. On April 23, 2022, Ms. Curtis drove to a nearby Chase Bank to see if she could submit her evidence of her conversation with the fraudsters for a faster result. The Chase Bank representative who spoke with Ms. Curtis informed her that there was nothing she could do for her. Later that day, Chase Bank informed Ms. Curtis that the $1,422 check she previously deposited was fraudulent and withdrew $1,422 from Ms. Curtis's account as well as a $12 bounced check fee.[22]

106. At some point before April 28, 2022, Ms. Curtis received a notification from Chase Bank that they were unable to retrieve her funds. Chase Bank provided no explanation, no findings of its investigation, or any information suggesting that Chase Bank undertook any investigation of Ms. Curtis' error reporting.

107. On information and belief, Zelle was already on notice of Ms. Curtis's claim based on information provided by Chase Bank. Despite Zelle having received notice of the error and/or unauthorized electronic fund transfer on Ms. Curtis' account, upon information and belief, Zelle failed to conduct any investigation of the error reporting.

108. Ms. Curtis closed her particular checking account with Chase Bank, and then opened a new checking account, for fear of being targeted again by the fraudsters.

109. Before closing the checking account at issue, Ms. Curtis was forced to transfer funds from her saving account with Chase Bank to her checking account in order to avoid a fee for a negative balance of over $1,000.

110. Within a week of contacting Chase Bank to make the dispute, Ms. Curtis also attempted to communicate with Zelle directly about the dispute. Specifically, Ms.

[22] Two $12 bounced check fees were ultimately refunded by Chase Bank on or about August 24, 2022.

Curtis visited the customer service page for Zelle, and after selecting the option for Zelle accounts through a bank, Ms. Curtis was directed to contact her bank relating to the Zelle account. Finding this to be unsatisfactory, Ms. Curtis then selected the option for accounts directly with Zelle, at which time Zelle electronically asked Ms. Curtis questions about her account that frustratingly did not go anywhere because Ms. Curtis did not have an account directly with Zelle.

111. Ms. Curtis has submitted a claim with her district attorney's office on or about May 20, 2022 and with the CFPB on or about July 19, 2022, concerning the Zelle fraud.

112. To date, Defendants have refused to refund Plaintiff the total amounts of $1,900 that were fraudulently extracted from Plaintiff's Chase Bank account.

CLASS ALLEGATIONS

113. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

114. Plaintiff is a member of and seeks to represent a Nationwide Class, pursuant to Fed. R. Civ. P. 23(b)(2) and/or (b)(3), defined as:

> **Nationwide Class**: All Chase Bank customers within the United States whose bank accounts with Chase Bank were debited via one or more transactions using the Chase Bank and/or Zelle mobile application and were not permanently credited by Defendant/s in full within 45 days of a dispute by the customer and/or their authorized representative concerning the transaction(s).

115. Plaintiff is also a member of and seeks to represent a New York Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and/or (b)(3), defined as:

> **New York Sub-Class**: All Chase Bank customers residing in New York whose bank accounts with Chase Bank were debited via one or more transactions using the Chase Bank and/or Zelle mobile application and were not permanently

> credited by Defendant/s in full within 45 days of a dispute by the customer and/or their authorized representative concerning the transaction(s).

116. Excluded from the Nationwide Class and Sub-Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Further excluded from the Nationwide Class and Sub-Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

117. Plaintiff reserves the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional sub-classes as warranted by additional investigation.

118. The proposed Nationwide Class and Sub-Class meet the criteria for certification under Rule 23(a), (b)(2) and/or (b)(3).

119. **Numerosity:** The members of the Nationwide Class and Sub-Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, on information and belief, the Nationwide Class and Sub-Classes consists of thousands of individuals nationwide.

120. Commonality: There are questions of law and fact common to the Nationwide Class and Sub-Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Plaintiff and the Class Members lost money that was transferred from their account via Zelle;

b. Whether Plaintiff and the Class Members were customers of Chase Bank at the time of the unauthorized transactions;

c. Whether Plaintiff and the Class Members were customers of Zelle at the time of the unauthorized transactions;

d. Whether Defendants violated EFTA by failing to adequately investigate the disputes of Plaintiff and the Class Members;

e. Whether Defendants violated EFTA by failing to correct errors on the accounts of Plaintiff and the Class Members within 45 days of the transactions being disputed;

f. Whether the transactions at issue were unauthorized EFTs, by way of a third party fraudulently obtaining access to Plaintiff's and the Class Members' accounts through fraudulent inducement, making them errors subject to EFTA's remedial provisions, including Regulation E;

g. Whether Plaintiff and the Class Members are entitled to maximum statutory damages, costs, and fees under EFTA;

h. Whether Defendants' conduct violated the state statutory claims alleged herein;

i. Whether Defendants breached their covenant of good faith and fair dealing owed to Plaintiff and the Class Members;

j. Whether Zelle was negligent in its actions and/or omissions;

k. Whether Defendants have been conferred an enrichment by keeping funds that they were obligated to replace pursuant to Regulation E's error resolution obligations; and

l. Whether Plaintiff and the Class Members are entitled to injunctive relief for Defendants' current and prospective conduct.

121. Typicality: Plaintiff's claims are typical of those of other members of the Nationwide Class and Sub-Class because Plaintiff was a victim of the Zelle scam by a third party who caused a withdrawal of funds from their Chase Bank account to occur through the Chase Bank/Zelle mobile application. After disputing that unauthorized transaction, Plaintiff was informed by Chase Bank that the transaction would ultimately not be reversed.

122. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and protect the interests of members of the Nationwide Class and Sub-Class. Plaintiff's Counsel is competent and experienced in litigating consumer class actions.

123. **Predominance:** Defendants have engaged in a common course of conduct toward Plaintiff as well as the members of the Nationwide Class and Sub-Class, in that all were induced into allowing a third party to make unauthorized withdrawals on their Chase Bank accounts using Zelle. The common issues arising from Defendants' conduct affecting members of the Nationwide Class and Sub-Class set out above predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

124. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most members of the Nationwide Class and Sub-Class would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual members of the Nationwide Class and Sub-Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Nationwide Class and Sub-Class, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

125. Defendants have acted on grounds that apply generally to the Nationwide Class and Sub-Class, so that class certification is appropriate.

126. All Members of the proposed Nationwide Class and Sub-Classes are readily

ascertainable. Defendants have access to consumer reporting of fraudulent and/or unauthorized transactions on their books and records. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

127. **Notice:** Plaintiff anticipate providing direct notice to the members of the Nationwide Class and Sub-Class for purposes of class certification, via U.S. Mail and/or email, based upon Defendants' and/or Defendants' agents' records.

FIRST CAUSE OF ACTION
VIOLATION OF THE ELECTRONIC FUND TRANSFER ACT ("EFTA"), 15 U.S.C. §§ 1693, *ET SEQ.*

(On Behalf of All Plaintiff and the Nationwide Class Against All Defendants)

128. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further allege as follows:

129. Plaintiff brings this count on behalf of the nationwide class or, alternatively, on behalf of the state Sub-Class.

130. The Electronic Fund Transfer Act ("EFTA") and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 15 U.S.C. §§ 1693 *et seq*.; 12 C.F.R. 1005.3(a).

131. The purpose of EFTA is "to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems. The primary objective … however, is the provision of individual consumer rights." 15 U.S.C. §§ 1693(b).

132. The primary objective of EFTA is "the protection of individual consumers engaging in electronic fund transfers and remittance transfers." 12 C.F.R. § 1005.1(b).

133. Financial institutions have error resolution obligations in the event that a consumer notifies the financial institution of an error. 15 U.S.C. § 1693f; 12 C.F.R. § 1005.11.

134. Chase Bank is a financial institution. 15 U.S.C. § 1693a(9); 12 C.F.R. § 1005.2(i).

135. Zelle is an MPP and financial institution because it issues an access device and agrees with a consumer to provide electronic fund transfer services. 15 U.S.C. §1693a(9);12 C.F.R. § 1005.2(i).

136. "If a financial institution, within sixty days after having transmitted to a consumer pursuant to [15 U.S.C. § 1693d(a), (c), or (d)] or notification pursuant to [15 U.S.C. § 1693(d)] receives oral or written notice in which the consumer[:] (1) sets forth or otherwise enables the financial institution to identify the name and the account number of the consumer; (2) indicates the consumer's belief that the documentation, or, in the case of notification pursuant to [15 U.S.C. § 1693d(b)], the consumer's account, contains an error and the amount of such error; and (3) sets forth the reasons for the consumer's belief (where applicable) that an error has occurred," the financial institution is required to investigate the alleged error. 15 U.S.C. § 1693f(a); 12 C.F.R. § 1005.11.

137. After said investigation, the financial institution must determine whether an error has occurred and report or mail the results of such investigation and determination to the consumer within ten (10) business days. *Id.*

138. A financial institution that provisionally recredits the consumer's account for the amount alleged to be in error pending an investigation, however, is afforded forty-five (45) days after receipt of notice of error to investigate. *Id.* § 1693f(c).

139. Pursuant to the EFTA, an error includes "an unauthorized electronic fund transfer." *Id.* § 1693f(f).

140. An Electronic Fund Transfer ("EFT") is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. § 1693a(7); 12 C.F.R. 1005.3(b)(1). Accordingly,

Regulation E applies to any P2P or mobile payment transactions that meet the definition of EFT. 12 C.F.R. 1005.3(b)(1)(v); *id.*, Comment 3(b)(1)-1ii.

141. Unauthorized EFTs are EFTs from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. § 1693a(12); 12 C.F.R. 1005.2(m).

142. According to the CFPB and FDIC, when a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account, that transfer meets Regulation E's definition of an unauthorized EFT.[23]

143. In particular, Comment 1005.2(m)-3 of Regulation E explains that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through robbery or fraud. As such, when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.[24]

144. Here, Plaintiff and Class Members (1) were fraudulently induced by third-party scammers to transfer money through the Chase Bank/Zelle mobile app; (2) had third-party scammers directly initiate and conduct transfers of money from their Chase Bank accounts through Zelle; and/or (3) were fraudulently induced to provide information to third-party scammers who then used the information fraudulently obtained from Plaintiff and Class Members to make unauthorized EFTs from the bank accounts of Plaintiff and other Class Members. All three of these scenarios constitute unauthorized EFT under Regulation E.

145. After the unauthorized EFTs were made, the EFTs appeared on the bank statements of Plaintiffs and Class Members.

---

[23] *See supra*, notes 14, 15.
[24] *See supra,* note 14.

146. Plaintiff and the Class Members notified Chase Bank of these errors within sixty (60) days of their appearances on their accounts.

147. After receiving notice of the unauthorized EFTs on Plaintiff's account, Chase Bank nonetheless informed Plaintiff that it would deduct the full amount of all fraudulent transactions ($1,900) from Plaintiff's Chase Bank account because Chase Bank erroneously concluded that the unauthorized EFT "was processed according to the information you provided or was authorized."

148. Within a week of contacting Chase Bank to make the dispute, Ms. Curtis also attempted to communicate with Zelle directly about the dispute. Specifically, Ms. Curtis visited the customer service page for Zelle, and after selecting the option for Zelle accounts through a bank, Ms. Curtis was directed to contact her bank relating to the Zelle account. Finding this to be unsatisfactory, Ms. Curtis then selected the option for accounts directly with Zelle, at which time Zelle electronically asked Ms. Curtis questions about her account that frustratingly did not go anywhere because Ms. Curtis did not have an account directly with Zelle.

149. On information and belief, Chase Bank or its agent separately notified Zelle of the unauthorized transactions that injured Plaintiff and the Class Members.

150. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members were unable to reclaim funds that were fraudulently taken from their Chase Bank accounts within the authorized period for error resolution.

151. Upon information and belief, Defendants knowingly and willfully failed to fulfill their obligations to investigate Plaintiff's unauthorized transactions and instead summarily concluded that the transfers of funds via Zelle from accounts of Plaintiff and other Class Members were not in error; such conclusions could not reasonably have been drawn from the evidence available to the financial institutions at the time of the investigation. 15 U.S.C. § 1693f(e)(2). In a letter from Chase Bank dated April 29, 2022 to Ms. Curtis, Chase Bank stated in part: "As we discussed and

agreed, no action will be taken" and that "This inquiry is now resolved." However, that statement from Chase Bank was false, as Ms. Curtis did not agree that the claim was resolved and did not agree that Chase Bank should take no further action.

152. Chase Bank has sent a similar letter to at least one other consumer who had not agreed that the claim was closed or that no further action should be taken on the claim. On information and belief, Chase Bank has sent similar letters to many other consumers who submitted claims due to fraudulent or unauthorized Zelle transactions as a means to deter consumers from pressing the claim further.

153. In a letter from Chase Bank dated May 2, 2022 to Ms. Curtis, Chase Bank opined that the transaction "was processed according to the information you provided or was authorized."

154. Similarly, in a letter from Chase Bank dated May 5, 2022 to Ms. Curtis, Chase Bank opined that the transaction "was processed according to the information you provided or was authorized."

155. Upon information and belief, and in violation of their regulatory obligations under 12 C.F.R. § Pt. 205, Supp. I, Defendants limited their investigation of Plaintiff's claim to only the payment instructions.

156. Upon information and belief, Defendants intentionally determined that the unauthorized transfer of funds via Zelle from accounts of Plaintiff and Class Members were not in error due to, at least in part, the Bank's financial self-interest as a stakeholder in Zelle and for both Chase Bank and Zelle to avoid liability to Plaintiff and other Class Members for the unauthorized transfers pursuant to Regulation E.

157. Defendants, in their normal course of business, refuse to completely reverse or refund funds (including any related service charges incurred because of the unauthorized charges), to consumers consistent with their obligations under Regulation E, §1005.6.

158. As such, Plaintiff and Class Members are each entitled to (i) actual damages; (ii) treble damages; (iii) the lesser of $500,000.00 or one percent (1%) of the net worth of Chase Bank and Zelle; and (iv) reasonable attorneys' fees and costs. *Id.* §§ 1693f(e)(2), 1693m(a)(2)(B)-(3).

SECOND CAUSE OF ACTION
BREACH OF CONTRACT INCLUDING BREACH OF THE COVENANT OF GOOD FAITH AND FAIR DEALING

(Asserted on Behalf of Plaintiff, the Nationwide Class, and the New York Sub-Classes Against Defendant Chase Bank Only)

159. Plaintiff repeats and realleges the above allegations concerning Chase Bank as if fully set forth herein.

160. Plaintiff and members of the Nationwide Class contracted with Chase Bank for checking account services, as embodied in Agreement 1, Agreement 2, and Agreement 3.

161. Chase Bank breached the terms of its contracts with consumers when as described herein, Chase Bank failed to refund fraudulent or unauthorized transactions on the Zelle money transfer service and failed to reimburse accountholders for fraud-induced losses incurred using the Zelle service.

162. Further, under the law of each of the states where Chase Bank does business, an implied covenant of good faith and fair dealing governs every contract. The covenant of good faith and fair dealing constrains Chase Banks's discretion to abuse self-granted contractual powers.

163. This good faith requirement extends to the manner in which a party employs discretion conferred by a contract.

164. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a

contract are mutually obligated to comply with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

165. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes his conduct to be justified. A lack of good faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Other examples of violations of good faith and fair dealing are willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance.

166. Chase Bank breached the covenant of good faith and fair dealing when they failed to fairly investigate reported fraudulent transactions on the Zelle money transfer service, failed to reimburse accountholders for fraud-induced losses incurred using the Zelle service, and adopted an unfair and unreasonable definition of the term "unauthorized transaction."

167. Each of Chase Bank's actions were done in bad faith and were arbitrary and capricious.

168. Plaintiff and members of the Nationwide Class have performed all of the obligations imposed on them under the contract.

169. Plaintiff and members of the Nationwide Class have sustained monetary damages as a result of Chase Bank's breaches of the Agreement and covenant of good faith and fair dealing.

//

//

//

//

//

//

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT

(Asserted on Behalf of Plaintiff, the Nationwide Class, and the New York Sub-Classes Against All Defendants - In the Alternative to Breach of Contract)

170. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs excluding Paragraphs 13, 69, 79-91, and 159-169, and further allege as follows:

171. Plaintiff brings this count on behalf of the nationwide class or, alternatively, on behalf of the state Sub-Class.

172. Defendants have been conferred the benefit or enrichment by keeping funds that Defendants are otherwise obligated to replace for Plaintiff and all Class Members pursuant to Regulation E's error resolution obligations.

173. Defendants know and appreciate this benefit or enrichment and the detriment or impoverishment to Plaintiff and all Class Members.

174. It is inequitable for Defendants to retain the benefit or enrichment of keeping these funds when they know they are obligated, as financial institutions, to comply with Regulation E and credit Plaintiff's and all Class members' accounts for the amounts fraudulently taken.

175. Plaintiff and all Class Members have sustained a detriment or an impoverishment from Defendants' failure to remedy this inequity and are entitled to restitution for the unjust enrichment to Defendants.

176. Plaintiff and all Class Members are entitled to restitution and disgorgement of the funds unjustly retained by Defendants in the absence of any legal relief.

//

//

//

//

FOURTH CAUSE OF ACTION
NEGLIGENCE

(On Behalf of Plaintiff, the Nationwide Class, and the New York Sub-Class Against Defendant Early Warning Services, LLC Only)

177. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further allege as follows:

178. Plaintiff brings this count on behalf of the nationwide class or, alternatively, on behalf of the state Sub-Class.

179. Zelle owed Plaintiff and all Class members a duty to take reasonable steps to adequately warn of known risks and/or dangers associated with Zelle, and to take appropriate steps in response to a known scam involving the app to protect consumers from malicious third parties.

180. Zelle breached its obligations to Plaintiff and all Class Members and were otherwise negligent and/or reckless by at least:

a. Failing to properly warn Plaintiff and all Class Members of the risks and/or dangers associated with Zelle or informing consumers about the Zelle-related scams;

b. Failing to review account agreements and disclosures to ensure they do not attempt to diminish or limit consumers' rights under Regulation E;

c. Failing to take appropriate steps to avoid unauthorized transactions through Zelle in response to known scams and continuing with business as normal;

d. Failing to adequately investigate and document findings from the investigations of fraud-related EFT disputes of the unauthorized transactions made on the accounts of Plaintiffs and all Class Members using the Zelle payment platform;

e. Failing to implement appropriate and sufficient safeguards against scams of the nature alleged in the Complaint in light of the knowledge that those scams have been rampant across the country;

f. Permitting scammers to use Zelle's member banks to siphon funds of Plaintiffs' and all Class members' accounts using the Zelle payment platform;

g. Failing to reverse unauthorized transactions pursuant to Regulation E error resolution requirements following disputes of Plaintiffs and all Class Members despite Zelle's knowledge that the transactions were unauthorized as part of a scam that is well-known to Zelle; and

h. Failing to permanently reverse or refund unauthorized transactions upon a sufficient showing by Plaintiff and all Class Members that the transactions were unauthorized.

181. As a direct and proximate result of Zelle's breaches, Plaintiff and all Class Members lost funds and incurred unnecessary related charges.

182. Plaintiff and all Class Members are entitled to damages for their continuing and increased risk of fraud and their loss of money.

FIFTH CAUSE OF ACTION
NEW YORK GENERAL BUSINESS LAW §§ 349 and 350

(On Behalf of Plaintiff and the New York Sub-Class Against All Defendants)

183. Plaintiff realleges and incorporates herein by reference the allegations contained in all preceding paragraphs, and further allege as follows:

184. New York General Business Law § 349(a) prohibits "conduct of any business, trade or commerce or in the furnishing of any service in this state" that is a "[d]eceptive act[] or practice[]."

185. Similarly, New York General Business Law § 350 states prohibits "[f]alse advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state…"

186. In 1980, the New York Legislature added a private right of action in 1980 for any person who has been injured by reason of a violation of this consumer protection statute. *See* New York General Business Law § 349(h).

187. Defendants have engaged in consumer-oriented conduct in marketing, promoting and offering the Zelle service to consumers within New York for personal, family or household use.

188. As described above, Defendants' marketing of the Zelle service was materially misleading, including in suggesting that the Zelle service is safe and without risk. Zelle failed to disclose the pervasiveness of the risk of fraud.

189. Such representations and omissions (including omissions as to the frequency and nature of Zelle scams), which Plaintiff relied upon, are deceptive and misleading not only to reasonable consumers but also under the standard to protect the "vast multitude which includes the ignorant, the unthinking and the credulous." *See Mennen Co. v. Gillette Co.*, 565 F. Supp. 648, 655 (S.D.N.Y. 1983).

190. Defendants' materially misleading statements are not protected by the "rules and regulations of, and the statutes administered by, the federal trade commission or any official department, division, commission or agency of the United States…"

191. As a result of Defendants' conduct, Plaintiff and the New York Sub-Class Members have suffered injury.

192. Plaintiff and the New York Sub-Class Members are entitled to actual damages or fifty dollars, whichever is greater, injunctive relief, and attorneys' fees from Defendants. New York General Business Law § 349(h).

193. Additionally, pursuant to New York General Business Law § 349(h), Plaintiff and the New York Sub-Class Members are each entitled to treble damages up to one thousand dollars for Defendants' willful or knowing violations of New York General Business Law § 349(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff pray for relief and judgment against Defendants, and each of them, as follows:

- Class certification of this action;

- Appointment of Plaintiff as Class Representative;
- Appointment of Plaintiff's attorneys as Class Counsel;
- An award of actual damages, in an amount to be determined at trial;
- An award of treble damages against Defendants pursuant to the EFTA;
- An award of the lesser of $500,000.00 or one percent (1%) of the net worth of Defendants;
- Injunctive and other equitable relief against Defendants as necessary to protect the interests of Plaintiff and other Class and Sub-Class Members from Defendants' current and prospective conduct, and an order prohibiting Defendants from engaging in unlawful and/or unfair acts described above, including public injunctive relief;
- Disgorgement;
- An order of restitution from Defendants for unjust enrichment;
- An order declaring Defendants' conduct as unlawful;
- Costs of Suit;
- Pre and post-judgment interest;
- An award of reasonable attorneys' fees pursuant to, *inter alia*, 15 U.S.C. § 1693m(a)(2)(B)–(3) and New York General Business Law § 349(h), and the common fund doctrine; and
- Any other relief the Court may deem just and proper, including interest.

//

//

//

//

//

//

//

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of all others similarly situated, hereby demand a jury trial on all claims so triable.

Dated: December 5, 2022

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: /s/ *Abbas Kazerounian*

Abbas Kazerounian, Esq.
(NY Bar #: 5590104)
ak@kazlg.com
48 Wall Street, Suite 1100
New York, NY 10005
Telephone: (800) 400-6808
Fax: (800) 520-5523
ATTORNEY FOR PLAINTIFF

ADDITIONAL PLAINTIFF'S COUNSEL

KAZEROUNI LAW GROUP, APC
Jason A. Ibey, Esq. (*pro hac vice forthcoming*)
jason@kazlg.com
321 N Mall Drive, Suite R108
St. George, Utah 84790
Telephone: (800) 400-6808

KELLER ROHRBACK L.L.P.
Laura R. Gerber (*pro hac vice forthcoming*)
lgerber@kellerrohrback.com
Derek W. Loeser, NY Bar # 5543640
dloeser@kellerrohrback.com
Nathan L. Nanfelt (*pro hac vice forthcoming)*
nnanfelt@kellerrohrback.com
1201 Third Avenue, Suite 3200
Seattle, Washington 98122
Telephone: (206) 623-1900